DETAILED ACTION

1. Applicant's amendment filed on July 29, 2010 and November 18, 2010 and have been entered. Claims 9-13 and 30-34 are pending. Claims 1-8, 14-29, and 35-58 are cancelled by the applicant.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given by Mr. Etienne P. de Villiers on January 13, 2011. The applicant has agreed and authorized examiner to amend claim 32 to overcome the multiple dependent claims issue (See MPEP § 608.01(n)).

CLAIMS:

3. Please replace claim 32 as follows:

Claim 32. The computing device program product of claims 30 [[and 32]] <u>or 31</u> in which masking is a bitwise exclusive or operation carried out on binary values.

Response to Argument

4. Applicant's arguments filed July 29, 2010, with respect to the specification have been fully considered and are persuasive. Therefore the rejection under 35 USC 101 has been withdrawn.

Allowable Subject Matter

5. Claims 9-13 and 30-34 are allowed. The following is an examiner's statement of reasons for allowance: The prior art does not disclose a) obtaining the key and a random value r; b) obtaining a set of n random input values m.sub.in1, . . . m.sub.inn; c) defining a masked function by masking the defined cryptographic function with the value m.sub.in1^ . . . ^m.sub.inn; d) masking the key with the random value r to define the value mkey; e) obtaining a set of random values m1, . . . mn-1; f) defining

a value mn to be r^m.sub.in1^ . . . ^m.sub.inn^m1^ . . . ^mn-1; and g) sing the values m1, . . . , mn and mkey to define input for the masked function, as set forth in claims 9 and 30.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2438

TBT
January 15, 2011